PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-217896
(43)Date of publication of application : 02.08.2002

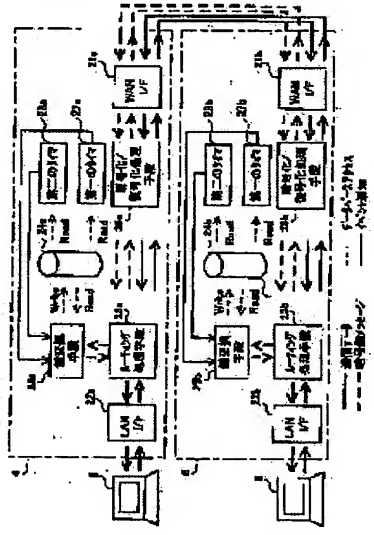
(51)Int.Cl. H04L 9/16
G06F 12/14
G09C 1/00
H04L 9/10

(21)Application number : 2001-015078
(22)Date of filing : 23.01.2001

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD
(72)Inventor : HOSHIDA MASAAKI

(54) METHOD FOR CIPHER COMMUNICATION AND GATEWAY DEVICE

(57)Abstract:
PROBLEM TO BE SOLVED: To secure the confidentiality and secrecy of communication data by exchanging a cryptographic key in a single session, while utilizing the standard protocols of the Internet, etc.
SOLUTION: The term of validity of a cryptographic key in a single session is defined. Then, a communication time is managed by using first timers 27a, 27b or the like. When the expiration of the validity of the cryptographic key comes near, key-exchanging means 25a and 25b performs the exchanging (delivering) processing of a new cryptographic key by using the security function of a wide-area network. When old cryptographic key information and new cryptographic key information coexist in SA database 24a and 24b, the newest cryptographic key information is selected by referring to a time stamp.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

[0003] At present, Ipsec is defined as a security protocol for the Internet by RFC(Request For Comment) which defines a standard protocol. Ipsec is made by adding encryption and authentication functions to IP (Internet Protocol), which is a fundamental protocol of the Internet. IKE (Internet Key Exchange) is also a defined protocol for exchanging keys necessary for encryption or authentication.

[0004] The gateway unit functions as an interface between a local network (such as in-house network or home network) and a wide area network such as the Internet, and it is generally complied with a cipher communication protocol. The use of the gateway unit (code gateway unit) having the encryption function can facilitate the cipher communication via the wide area network.

[0005] The encryption ensures the confidentiality and secrecy of short sessions.

[0006]

[The problems to be solved by the invention]

In order to secure the confidentiality and secrecy of session groups as constantly maintained virtual private lines or of sessions over a couple of hours such as movie distribution, it is necessary to update encryptions keys regularly.

[0007] However, communication channels used for temporary encryption of contents of the communication are released for the update of the encryptions keys. (the communication channels, i.e., key information including encryption key data, to be referred to as Security Association(SA) hereinafter) Therefore, the security of the communication is not guaranteed during a period where the encryption keys are updated, which degrades the confidentiality and secrecy of the communication data of the session.

[0008] Moreover, in a present situation that always-on connections in the networks have been widespread, there may be users' demand for securing the confidentiality by making key exchanges by every couple of hours while constantly maintaining movie stream application.

[0009] The current security function on the Internet cannot deal with exchanging the encryption keys in a single session. Changing the specification of the security function to update the encryption key during a single session is a way of solution, however, with generality of the wide area networks taken into consideration, it is a very hard thing to achieve.

[0010] The invention is achieved with the above regards taken into consideration. The object of the invention is to realize the encryption key exchange in a single session using a standard protocol of the Internet, and to secure the confidentiality and secrecy of communication data

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報**（Ａ）　(11)特許出願公開番号
特開2002－217896
（P2002－217896A）
(43)公開日　平成14年８月２日(2002.8.2)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード'（参考）
Ｈ０４Ｌ　9/16		Ｇ０６Ｆ　12/14	３２０Ｂ	５Ｂ０１７
Ｇ０６Ｆ　12/14	３２０		３２０Ｆ	５Ｊ１０４
		Ｇ０９Ｃ　1/00	６４０Ｚ	
Ｇ０９Ｃ　1/00	６４０	Ｈ０４Ｌ　9/00	６４３	
Ｈ０４Ｌ　9/10			６２１Ａ	

審査請求　未請求　請求項の数12　ＯＬ　（全 12 頁）

(21)出願番号　特願2001－15078(P2001－15078)

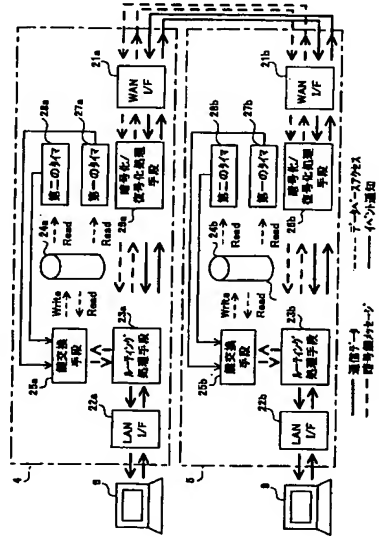
(22)出願日　平成13年１月23日(2001.1.23)

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地
(72)発明者　昼田　昌昭
神奈川県横浜市港北区綱島東四丁目３番１号　松下通信工業株式会社内
(74)代理人　100105050
弁理士　鷲田　公一

Ｆターム(参考)　5B017 AA03 AA06 BA07 BB09 BB10
5J104 AA01 AA11 AA16 AA34 EA04
EA17 NA02 PA07

(54)【発明の名称】　暗号通信方法およびゲートウエイ装置

(57)【要約】
【目的】　インターネット等の標準的なプロトコルを利用しつつ、１つのセッション中における暗号鍵の交換を可能として、通信データの機密性・秘匿性を確保すること。
【解決手段】　一つのセッション中における暗号鍵の有効期間を定めておく。そして、第１のタイマ２７ａ，２７ｂ等を用いて通信時間の管理を行う。暗号鍵の有効期間の満了が近づくと、鍵交換手段２５ａ，２５ｂが広域ネットワークのセキュリティ機能を利用して、新たな暗号鍵の交換（配送）処理を行う。ＳＡデータベース２４ａ，２４ｂに、旧暗号鍵情報と新暗号鍵情報とが併存している場合には、タイムスタンプを参照して最新の暗号鍵情報を選択する。



1

【特許請求の範囲】

【請求項１】　広域ネットワークを介して暗号通信を行う場合に、一つのセッションにおける暗号鍵の有効期間を定めておき、通信時間の管理を行ない、前記暗号鍵の前記有効期間の満了が近づくと、旧暗号鍵と新暗号鍵が一定時間並存するように、前記広域ネットワークのセキュリティ機能を利用して、新たな暗号鍵の交換処理を行うことを特徴とする暗号通信方法。

【請求項２】　旧暗号鍵と新暗号鍵が併存している場合には、最新の暗号鍵を選択して暗号化または復号化を行うようにしたことを特徴とする請求項１記載の暗号通信方法。

【請求項３】　暗号化処理を施したパケットを通信する暗号通信方法であって、

送信側と受信側の各々に鍵情報を格納する鍵情報データベースを設け、それぞれの鍵情報データベースを参照して鍵情報を取得し、暗号化および復号化を行うと共に、

前記鍵情報にはタイムスタンプが含まれるようにし、

予め、一つのセッションにおける前記鍵の有効期間を定めておき、

前記セッションの時間管理を実施し、前記セッションの時間が前記鍵の有効期間を越える場合には、前記鍵の有効期間の満了前の所定期間において、送信側から受信側に新たな鍵の配送処理を行って、受信側および送信側のそれぞれにおける前記鍵情報データベースに新たな鍵情報を構築し、

前記新たな鍵情報の構築により、前記セッションに対して古い鍵情報と新たな鍵情報とが併存することとなった場合に、前記鍵情報に含まれる前記タイムスタンプを参照して、最新のタイムスタンプを含む鍵情報を選択するようにし、

これにより、前記セッションの途中で、セッション時間の管理に基づく鍵情報の更新処理を行うようにしたことを特徴とする暗号通信方法。

【請求項４】　請求項３において、

前記鍵情報は少なくとも、暗号鍵および暗号化アルゴリズムの情報を有することを特徴とする暗号通信方法。

【請求項５】　請求項３において、

前記セッションに対する古い鍵情報について有効期間が満了した場合には、その古い鍵情報を、送信側および受信側の前記鍵情報データベースから削除することを特徴とする暗号通信方法。

【請求項６】　暗号化処理を施したパケットを通信する暗号通信方法であって、

送信側と受信側の各々に鍵情報を格納する鍵情報データベースを設け、それぞれの鍵情報データベースを参照して鍵情報を取得し、暗号化および復号化を行うと共に、

前記鍵情報には、送信先を特定するための情報と、暗号鍵および暗号アルゴリズムの情報と、タイムスタンプとが含まれるようにし、

2

予め、一つのセッションにおける前記鍵の有効期間を定めておき、

前記セッションの時間管理を実施し、前記セッションの時間が前記鍵の有効期間を越える場合には、前記鍵の有効期間の満了前の所定期間において、送信側から受信側に新たな鍵の配送処理を行って、受信側および送信側のそれぞれにおける前記鍵情報データベースに新たな鍵情報を構築し、

送信側が暗号化されたパケットを送信する場合には、送信先を特定するための情報をキーとして、送信側の前記鍵情報データベースを検索して該当する鍵情報を取得するものとし、前記鍵情報データベースの検索の結果として該当する鍵情報が２以上存在した場合には、タイムスタンプを参照して最新の鍵情報を選択するようにし、選択された鍵情報に含まれる前記暗号鍵および暗号アルゴリズムの情報を用いて送信パケットの暗号化を行うと共に、前記選択された鍵情報を示す識別番号を前記送信パケットのヘッダに記載して、その送信パケットを受信側に送信し、

受信側では、送られてきたパケットのヘッダに記載されている前記鍵情報を示す識別番号を参照して、受信側における前記鍵情報データベースを検索し、前記識別番号に該当する鍵情報を取得し、その鍵情報に含まれている前記暗号鍵および暗号アルゴリズムの情報を用いて、パケットの復号化を行なうようにし、

これにより、一つのセッションの途中で、セッション時間の管理に基づく鍵情報の更新処理を行うことを可能としたことを特徴とする暗号通信方法。

【請求項７】　広域ネットワークを介した暗号通信を行う機能をもつ暗号ゲートウエイ装置であって、

前記広域ネットワークを介して暗号鍵情報を交換するための鍵交換手段と、

暗号鍵に関する情報を蓄積する暗号鍵データベースと、

暗号鍵の有効期限までの残り時間が所定時間以下となったことを検出して、前記鍵交換手段に通知するタイマと、

前記暗号鍵データベースを参照して必要な暗号鍵情報を取得し、その暗号鍵情報を用いて暗号化および復号化を行う暗号化／復号化手段と、を具備し、

前記鍵交換手段は、前記タイマからの通知を受けると、通信先から新たな暗号鍵情報を入手して前記暗号鍵データベースに登録し、

また、前記暗号化／復号化手段は、前記暗号鍵データベースを参照した結果、一つのセッションに関して２以上の暗号鍵情報が存在する場合には、最新の暗号鍵情報を用いて暗号化または復号化を行うことを特徴とするゲートウエイ装置。

【請求項８】　広域ネットワークを介した暗号通信を行う機能をもつゲートウエイ装置であって、

前記広域ネットワークを介して暗号鍵情報を交換するた

めの鍵交換手段と、
暗号鍵に関する情報を蓄積する暗号鍵データベースと、
暗号鍵の有効期限までの残り時間が所定時間以下となったことを検出して、前記鍵交換手段に通知する第１のタイマと、
暗号鍵の有効期限が満了したことを検出して、前記鍵交換手段に通知する第２のタイマと、
前記暗号鍵データベースを参照して必要な暗号鍵情報を取得し、その暗号鍵情報を用いて暗号化および復号化を行う暗号化／復号化手段と、を具備し、
前記鍵交換手段は、前記第１のタイマから通知を受けると、通信先との間で暗号鍵情報の交換を行って、前記通信先の前記暗号鍵データベースに新たな鍵情報を登録させ、また、前記第２のタイマから通知を受けると、通信先との間でメッセージの交換を行って、前記通信先の前記暗号鍵データベースから、有効期間が満了した暗号鍵情報を削除させ、
また、前記暗号化／復号化手段は、一つのセッションに関して２以上の暗号鍵情報が存在する場合には、最新の暗号鍵情報を用いて暗号化または復号化を行うことを特徴とするゲートウエイ装置。
【請求項９】　請求項７または請求項８において
前記暗号化／復号化手段は、ＩＰ（Ｉｎｔｅｒｎｅｔ Ｐｒｏｔｏｃｏｌ）における認証ヘッダ（Ａｕｔｈｅｎｔｉｃａｔｉｏｎ Ｈｅａｄｅｒ）に準じる、もしくは同等の手段とアルゴリズムで、認証値算出処理または改ざん検出処理を行うことを特徴とするゲートウエイ装置。
【請求項１０】　請求項７または請求項８において、
前記の暗号化処理を施す暗号化／復号化手段は、ＩＰ（Ｉｎｔｅｒｎｅｔ Ｐｒｏｔｏｃｏｌ）における暗号ペイロード（Ｅｎｃａｐｓｕｌａｔｉｏｎｇ Ｓｅｃｕｒｉｔｙ Ｐａｙｌｏａｄ）に準じる、もしくは同等の手段とアルゴリズムで、暗号化処理または復号化処理を行うことを特徴とするゲートウエイ装置。
【請求項１１】　広域ネットワークを介した暗号通信を行う機能をもつゲートウエイ装置であって、
前記広域ネットワークを介して暗号鍵情報を交換するための鍵交換手段と、
暗号鍵に関する情報を蓄積する暗号鍵データベースと、
暗号鍵の有効期限までの残り時間が所定時間以下となったことを検出して、前記鍵交換手段に通知するタイマと、
前記暗号鍵データベースを参照して必要な暗号鍵情報を取得し、その暗号鍵情報を用いて暗号化および復号化を行う暗号化／復号化手段と、を具備し、
前記鍵交換手段は、前記タイマからの通知を受けると、通信先との間で暗号鍵情報の交換を行い、前記通信先の前記暗号鍵データベースに新たな鍵情報を登録させて暗号鍵情報の更新処理を行い、

前記暗号化／復号化手段は、送信パケットの暗号化を実行する場合には、まず、通信先を特定するための情報をキーとして、前記鍵情報データベースを検索して該当する鍵情報を取得し、前記鍵情報データベースの検索の結果として該当する鍵情報が２以上存在した場合には、前記鍵情報に含まれるタイムスタンプを参照して最新の鍵情報を選択するようにし、選択された鍵情報に含まれる暗号鍵および暗号アルゴリズムの情報を用いて送信パケットの暗号化を行うと共に、前記選択された鍵情報を示す識別番号を前記送信パケットのヘッダに記載し、
また、前記暗号化／復号化手段は、受信したパケットの復号化処理を行う場合には、受信パケットのヘッダに記載されている前記鍵情報を示す識別番号を参照して、前記鍵情報データベースを検索し、前記識別番号に該当する暗号鍵情報を取得し、その暗号鍵情報に含まれている前記暗号鍵および暗号アルゴリズムの情報を用いて、パケットの復号化を行なうようにし、
これにより、一つのセッションの途中で、セッション時間の管理に基づく鍵情報の更新処理を行うことを可能としたことを特徴とするゲートウエイ装置。
【請求項１２】　コンピュータを、
暗号鍵に関する情報を蓄積する暗号鍵データベースと、
暗号鍵の有効期限までの残り時間が所定時間以下となったことを検出するタイマと、
前記広域ネットワークを介して暗号鍵情報を交換する機能を有し、かつ、前記タイマからの通知を受けると、通信先との間で暗号鍵情報の交換を行って前記暗号鍵データベースに新たな鍵情報を登録する鍵交換手段と、
前記暗号鍵データベースを参照して必要な暗号鍵情報を取得し、その暗号鍵情報を用いて暗号化および復号化を行い、かつ、暗号鍵情報が存在する場合には、最新の暗号鍵情報を用いて暗号化または復号化を行う暗号化／復号化手段と、
を具備する暗号ゲートウエイ装置として機能させるためのプログラムを記録していることを特徴とする記録媒体。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、通信内容の盗聴や改竄を防止するために転送データを暗号化し、ネットワークを介して通信する、暗号通信方法およびゲートウエイ装置に関する。
【０００２】
【従来の技術】ネットワークを介してデータ交換を行う通信システムにおいては、盗聴者に転送データの盗聴・改竄を行わせないために、通信内容を暗号化したり、データの完全性をチェックする情報を付加するなどして、セキュリティ機能を強化してきた。
【０００３】現在、インターネットにおいては、標準プロトコルを規定するRFC(Request For Comment)にて、イ

ンターネットの基盤を担うプロトコルであるIP(Internet Protocol)に暗号化や認証機能を付加したIPsecが、セキュリティプロトコルとして規定されている。併せて、暗号化や認証に必要な鍵交換を行うプロトコルであるIKE(Internet Key Exchange)も規定されている。

【０００４】ローカルネットワーク（構内ネットワークやホームネットワーク等）と、インターネットのような広域ネットワークとの間のインタフェースとして機能するゲートウエイ装置は、暗号通信プロトコルに対応しているのが通常であり、暗号機能をもつゲートウエイ装置（暗号ゲートウエイ装置）を用いれば、広域ネットワークを介した暗号通信を容易に行うことができる。

【０００５】暗号化を行うことによって、短時間のセッションに対する機密性・秘匿性が確保されることになる。

【０００６】

【発明が解決しようとする課題】例えば、仮想専用線として定常的に維持されるセッション群や、数時間に及ぶ映像配信のようなセッションに対する機密性・秘匿性の確保には、暗号鍵の定期的な更新が必要となる。

【０００７】しかしながら、暗号鍵の更新の際には、一時的に通信内容を暗号化するための通信チャネル（暗号化鍵のデータを含む鍵情報；以下、Security Association:SAと呼ぶ）が解放される。よって、暗号鍵を更新している期間のセキュリティは保証されないことになり、そのセッションに対する通信データの機密性・秘匿性が低下する。

【０００８】さらに、ネットワークの常時接続サービスが普及しつつある昨今においては、映像ストリーム系アプリケーションを定常的に維持しつつ、数時間という単位での鍵交換による秘匿性の確保が、ユーザ側からの要望としてあるものと考えられる。

【０００９】現状のインターネットのセキュリティ機能は、１つのセッション中に暗号鍵を交換することには対応できていない。１つのセッション中に暗号鍵を更新するために、セキュリティ機能の規格を変更することも考えられるが、広域ネットワークの汎用性を考慮すると、多くの困難が予想される。

【００１０】本発明は、このような考察に基づいてなされたものであり、その目的は、インターネット等の標準的なプロトコルを利用しつつ、１つのセッション中における鍵交換を可能として、通信データの機密性・秘匿性を確保することにある。

【００１１】

【課題を解決するための手段】本発明では、一つのセッションにおける暗号鍵の有効期間を定めておき、通信時間の管理を行ない、暗号鍵の有効期間の満了が近づくと、広域ネットワークのセキュリティ機能を利用して、新たな暗号鍵の交換（配送）処理を行う。そして、旧暗号鍵と新暗号鍵が併存している場合には、最新の暗号鍵を選択することとする。

【００１２】これにより、１つのセッション中において、スムーズな暗号鍵の更新を実現できる。また、通信時間の管理を行うと共に、暗号化鍵が併存する場合には、最新のものを選ぶという簡単な機能を付加するだけでよいため、実現が容易である。

【００１３】本発明の暗号通信方法の一つの態様では、送信側と受信側の各々に鍵情報を格納する鍵情報データベースを設け、それぞれの鍵情報データベースを参照して鍵情報を取得し、暗号化および復号化を行うと共に、前記鍵情報にはタイムスタンプが含まれるようにし、予め、一つのセッションにおける前記鍵の有効期間を定めておき、前記セッションの時間管理を実施し、前記セッションの時間が前記鍵の有効期間を越える場合には、前記鍵の有効期間の満了前の所定期間において、送信側から受信側に新たな鍵の配送処理を行って、受信側および送信側のそれぞれにおける前記鍵情報データベースに新たな鍵情報を構築し、前記新たな鍵情報の構築により、前記セッションに対して古い鍵情報と新たな鍵情報とが併存することとなった場合に、前記鍵情報に含まれる前記タイムスタンプを参照して、最新のタイムスタンプを含む鍵情報を選択するようにする。これによって、セッションの途中で、セッション時間の管理に基づく鍵情報の更新処理をスムーズに行うことができる。

【００１４】

【発明の実施の形態】以下、本発明の実施の形態について、図面を参照して説明する。

【００１５】図２は、本発明を適用する暗号通信システムの全体構成を示す図である。図２において、広域ネットワーク１（Ｗｉｄｅ　Ａｒｅａ　Ｎｅｔｗｏｒｋ：ＷＡＮと記載する）は、離れた拠点間の構内ネットワークを接続し、異なる拠点間でデータの交換が行われている通信ネットワークである。

【００１６】構内ネットワーク２，３（以下、Ｌｏｃａｌ　Ａｒｅａ　Ｎｅｔｗｏｒｋ：ＬＡＮと呼ぶ）はパーソナルコンピュータやワークステーションなどの通信端末やブリッジ、スイッチなどの様々な通信機器が同軸ケーブルにより接続されており、構内の通信端末間や構内の通信端末と異なる拠点の通信端末との間のデータの交換が行われている通信ネットワークである。なお、本実施の形態では、構内ネットワークを例にして説明するが、これに限定されるものではない。例えば、家庭内に構築されるホームネットワークでもよい。

【００１７】ゲートウェイ装置４，５は、例えば、ＬＡＮ２に接続された通信端末から、離れた拠点のＬＡＮ３に接続された通信端末へデータを送る際に、ＬＡＮとＷＡＮとを接続するルータ、ターミナルアダプタなどのインタフェース装置である。ゲートウエイ装置４，５は、暗号化／復号化機能を有する暗号ゲートウエイ装置である。

【００１８】また、通信端末６，７，８，９，１０，１１は、ＬＡＮやＷＡＮを介してデータの交換を行うパーソナルコンピュータやワークステーションなどである。傍受端末１２は、ＬＡＮを介してデータ交換を行う通信端末間の通信データを、そのデータが転送される途中で傍受して通信内容を解読する機能を有するパーソナルコンピュータやワークステーションなどである。

【００１９】次に、ゲートウエイ装置の基本的な構成について、図１を用いて説明する。図１は、ゲートウェイ装置４，５の内部構成例を示す図である。図１のシステムでは、端末６と、端末９との間で暗号通信を行うものとする。

【００２０】図示されるように、ゲートウェイ装置４，５はそれぞれ、ＷＡＮとの間でデータのやりとりを行うＷＡＮインタフェース２１ａ，２１ｂと、ＬＡＮとの間でデータのやりとりを行うＬＡＮインタフェース２２ａ，２２ｂと、通信データが格納されているパケットのヘッダ内部の宛先アドレスにより転送先を決定するルーティング処理手段２３ａ，２３ｂとを有する。

【００２１】さらに、ゲートウェイ装置４，５はそれぞれ、セッション毎の暗号化アルゴリズムと暗号鍵が格納されているセキュリティアソシエーション・データベース（ＳＡデータベース）２４ａ，２４ｂと、セッション毎の暗号化アルゴリズムと暗号鍵を送信元、もしくは送信先ゲートウェイと折衝し、その情報をＳＡデータベース２４ａ，２４ｂに書き込む鍵交換手段２５ａ，２５ｂを有する。

【００２２】また、さらに、ゲートウェイ装置４，５はそれぞれ、ＷＡＮインタフェース２１ａ，２１ｂを介して通信するパケットに対して、当該ゲートウェイ装置からＷＡＮへ送信するパケットについては、ＳＡデータベース２４ａ，２４ｂに基づき暗号化処理行い、一方ＷＡＮから当該ゲートウェイ装置が受信したパケットについては、ＳＡデータベースに基づき復号化処理を行う暗号化／復号化処理手段２６ａ，２６ｂを有する。

【００２３】また、さらに、ゲートウェイ装置４，５はそれぞれ、セッション毎のＳＡの有効時間を管理し、有効時間満了を契機としてＳＡ解放を鍵交換手段２５ａ，２５ｂへ通知する第１のタイマ２７ａ，２７ｂと、セッション毎のＳＡの有効時間を管理し、有効時間満了に先立って、ＳＡ確立を鍵交換手段２５ａ，２５ｂへ通知する第２のタイマ２８ａ，２８ｂを有する。

【００２４】また、図１において、太い実線は通信データを示し、太い点線は暗号鍵メッセージを示し、細い実線はイベント通知を示し、細い点線はデータベースアクセスを示す。

【００２５】以下、図１に示すゲートウエイ装置を用いた、暗号通信動作について説明する。図３に、主要な手順（の概要）をまとめて示している。

【００２６】つまり、図３に記載されるように、暗号通信を行うに際して、まず、送信側では、暗号鍵情報のチャネルであるセキュリティアソシエーション（ＳＡ）を確立し（つまり、暗号鍵の交換処理を行い）、送信側のＳＡデータベースに鍵情報を書き込む（ステップ４０）。

【００２７】次に、送信側では、送信先の情報をキーとして自己のＳＡデータベースを検索して、合致するＳＡ情報（暗号鍵，暗号化アルゴリズム，タイムスタンプを含む暗号鍵情報）を探し出し、該当する暗号鍵と暗号化アルゴリズムを用いて、送信データ（送信パケット）を暗号化して送信する。このとき、送信パケットのヘッダの一部に、ＳＡの識別情報（ＳＡＩＤ）を記載する。受信側では、パケットのヘッダに記載されているＳＡＩＤを参照して、自己のＳＡデータベースを検索し、暗号化鍵情報を取得し、受信データの復号化を行う（ステップ４１）。

【００２８】セッションが開始されると、送信側にて、第１のタイマを用いたＳＡの有効期限管理（暗号鍵情報の有効期限の管理）を行い、期限の満了前の所定の時間となると、第１のタイマが鍵交換手段にこれを通知する（ステップ４２）。

【００２９】通知を受けた鍵交換手段は、ＳＡを再度、確立し、これにより、送信側および受信側双方のＳＡデータベースに新たな暗号鍵情報が記録され、ＳＡデータベースが更新される（ステップ４３）。

【００３０】そして、送信側では、送信先の情報およびタイムスタンプをキーとしてＳＡデータベースを検索する。このとき、一つのセッションに対して、ＳＡデータベース中に２つ（２以上）のＳＡ情報（暗号鍵情報）が存在するときは、タイムスタンプが最新のものを選ぶという条件の下で、ＳＡデータベースを検索する。そして、合致する暗号鍵と暗号化アルゴリズムを用いて送信データを暗号化し、送信パケットのヘッダに鍵情報の識別番号（ＳＡＩＤ）を記載して送信する。受信側では、パケットのヘッダに記載されているＳＡＩＤを参照して、復号化を行う（ステップ４４）。そして、古い暗号鍵の有効期間が満了すると、ＳＡを解放して古い暗号鍵情報を削除する・つまり、一つのセッションにおける暗号鍵の有効期間を定めておき、通信時間の管理を行ない、暗号鍵の有効期間の満了が近づくと、広域ネットワークのセキュリティ機能を利用して、新たな暗号鍵の交換（配送）処理を行う。そして、旧暗号鍵と新暗号鍵が併存している場合には、送信側にて最新の暗号鍵を選択して暗号化を行い、その暗号化鍵のＩＤ（ＳＡＩＤ）をパケットに添付するだけである。受信側では、従来とまったく同じように、ＳＡＩＤを参照してＳＡデータベースを検索して復号化を行えばよい。

【００３１】これにより、１つのセッション中において、スムーズな暗号鍵の更新を実現できる。また、通信時間の管理を行うと共に、暗号化鍵が併存する場合に

は、最新のものを選ぶという簡単な機能を付加するだけでよいため、実現がきわめて容易である。

【００３２】図４に示すように、本実施の形態では、一つのセッション中において、最初は”ＳＡＩＤ１”の暗号鍵情報が有効である。そして、暗号鍵の有効期限である時刻ｔ２より、一定時間Ｔ１だけ前の時点ｔ１になると、新たなＳＡが確立されて”ＳＡＩＤ３”の暗号鍵情報が有効となる。この時点で、”ＳＡＩＤ１”の暗号鍵情報は、ＳＡデータベースには存在するものの、暗号化／復号化には使用されず、実質的に無効な状態となる。そして、時刻ｔ２になると、古いＳＡは解放されて、”ＳＡＩＤ１”の暗号鍵情報はＳＡデータベースより削除される。このようにして、一つのセッション中において、スムーズに、しかも簡単に、暗号鍵の切り換えを行うことができる。

【００３３】以下、図１，図５，図６および図７～図９を用いて、より具体的に説明する。

【００３４】図７（ａ），図８（ａ），図９（ａ）は、本実施の形態における、パケット送信側ゲートウェイ装置の暗号化処理に必要となるＳＡデータベースの中身を示すものである。図７（ａ）は、セッション開始当初のＳＡ情報であり、図８（ａ）は、暗号鍵の有効期間の満了が近づいてきて、新たなＳＡと古いＳＡが併存している状態におけるＳＡ情報であり、図９（ａ）は、古い暗号鍵の有効期間が満了して、古いＳＡが解放された状態におけるＳＡ情報を示している。

【００３５】図示されるように、ＳＡ情報（暗号鍵情報）は、セキュリティアソシエーション（暗号鍵に関する情報）を識別するＳＡＩＤ、送信元アドレス、送信元ポート番号、送信先アドレス、送信先ポート番号、暗号化アルゴリズム、暗号鍵、タイムスタンプで構成される。

【００３６】また、図７（ｂ），図８（ｂ）、図９（ｂ）は、本発明の実施の形態におけるパケット受信側ゲートウェイ装置の復号化処理に必要となるＳＡデータベースの内容（ＳＡ情報）であり、それぞれ、図７（ａ），図８（ａ），図９（ａ）に対応している。ＳＡ情報は、セキュリティアソシエーションを識別するＳＡＩＤ、暗号化アルゴリズム、暗号鍵を含んで構成されている。

【００３７】本実施の形態において、図７（ａ），（ｂ）におけるＳＡデータベースは、送信元アドレス、送信元ポート番号、送信先アドレス、送信先ポート番号、暗号化アルゴリズムを保守手順により初期設定した後、ゲートウェイ装置４，５における鍵交換手段により交換されたＳＡＩＤ、暗号鍵、その時点でのタイムスタンプにより構築されたものとする。

【００３８】次に、図１に示される端末６から端末９に対して確立されたセッションにおいて、端末６から端末９へ送信される通信データの暗号化と復号化の一連の流れを具体的に説明する。

【００３９】図１において、端末６から端末９への宛先アドレス、当該セッションに対応したポート番号が指定され、送信されたパケットは、構内ネットワーク２を介して、ゲートウェイ装置４に到着する。

【００４０】パケットは、ゲートウェイ装置４において、ＬＡＮインタフェース２２ａを経由し、ルーティング処理手段２３ａにより広域ネットワーク１へ転送するパケットと判断され、暗号化／復号化処理手段２６ａへ転送される。

【００４１】暗号化／復号化処理手段２６ａにおいては、図７（ａ）におけるＳＡデータベースを参照し、前記パケットのヘッダ部分に記載されている送信先アドレスと送信先ポート番号をキーに一致するＳＡを検索し、そのＳＡの暗号化アルゴリズムと暗号鍵により暗号化を行い、ヘッダの一部に該当するＳＡＩＤを記載する。その後、パケットは暗号化／復号化処理手段２６ａからＷＡＮインタフェース２１ａを経由して、広域ネットワーク１へ転送される。

【００４２】さらに、パケットはゲートウェイ装置５へ転送され、ＷＡＮインタフェース２１ｂを介して、暗号化／復号化処理手段２６ｂへ転送される。暗号化／復号化処理手段２６ｂにおいては、図６におけるＳＡデータベースを参照し、受信したパケットのヘッダに記載されたＳＡＩＤと一致するＳＡを検索し、そのＳＡの暗号化アルゴリズムと暗号鍵により復号化を行う。

【００４３】その後、前記パケットは暗号化／復号化処理手段２６ｂからルーティング処理手段２３ｂとＬＡＮインタフェース２２ｂを経由し、構内ネットワーク３を介して端末９に転送される。

【００４４】このように、ゲートウェイ装置４，５との間で暗号化／復号化処理が施されることにより、広域ネットワーク１において暗号化通信が実現される。これにより、傍受端末１２に対する機密性・秘匿性を確保する。

【００４５】次に、端末６から端末９のセッションに対するＳＡ有効時間満了に先立ち、そのセッションに対する新たなＳＡを確立し、その後の通信データの暗号化と復号化の一連の流れを説明する。

【００４６】ゲートウェイ装置４における第２のタイマ２８ａは、ＳＡデータベース２４のセッション毎のタイムスタンプを定期的に参照し、ＳＡのタイムスタンプと固定的なＳＡの有効時間と現在の時刻とにより、ＳＡの有効時間満了までの残余時間が一定時間以下であった場合に、そのＳＡの送信元アドレス、送信元ポート番号、送信先アドレス、送信先ポート番号、暗号化アルゴリズムを含むＳＡ確立指示を鍵交換手段２５ａへ通知する。

【００４７】鍵交換手段２５ａは、セッション鍵交換手順に基づくメッセージを生成した後、パケットヘッダの宛先アドレスに対向となるゲートウェイアドレス（この

場合、ゲートウェイアドレスは、ゲートウェイ装置５となる）を記載し、ルーティング処理手段２３ａと暗号化／復号化処理手段２６ａとＷＡＮインタフェース２１ａを経由して、広域ネットワーク１に転送される。（なお、暗号化／復号化処理手段２６ａにおいては、必ずしも暗号化されなくてもよい。）さらに、前記セッション鍵交換手順に基づくメッセージを含むパケットはゲートウェイ装置５へ転送され、ＷＡＮインタフェース２１ｂ、暗号化／復号化処理手段２６ｂとルーティング処理手段２３ｂを介して、鍵交換手段２５ｂへ転送され、セッション鍵交換手順に基づき、そのセッションに対する新たなＳＡが確立され、ゲートウェイ装置４、５のＳＡデータベースは、図８（ａ），（ｂ）へと更新される。

【００４８】その後、端末６から端末９への宛先アドレス、そのセッションに対応したポート番号が指定され、送信されたパケットは、先に説明した動作により、構内ネットワーク２を介してゲートウェイ装置４に到着する。

【００４９】パケットは、ゲートウェイ装置４において、ＬＡＮインタフェース２２ａを経由し、ルーティング処理手段２３ａにより広域ネットワーク１へ転送するパケットと判断され、暗号化／復号化処理手段２６ａへ転送される。暗号化／復号化処理手段２６ａにおいては、図８（ａ）におけるＳＡデータベースを参照し、パケットのヘッダ部分に記載されている「送信先アドレス」と「送信先ポート番号」と一致するＳＡであり、かつ、「タイムスタンプが最新であるＳＡ」を検索し、そのＳＡの暗号化アルゴリズムと暗号鍵により暗号化を行い、ヘッダの一部に該当するＳＡＩＤを記載する。

【００５０】その後、先に説明したのと同様な動作により、パケットはゲートウェイ装置５へ転送され、ＷＡＮインタフェース２１ｂを介して、暗号化／復号化処理手段２６ｂへ転送される。

【００５１】暗号化／復号化処理手段２６ｂにおいては、図８（ｂ）におけるＳＡデータベースを参照し、先に説明した動作と同様に、受信したパケットのヘッダに記載されたＳＡＩＤと一致するＳＡを検索し、当該ＳＡの暗号化アルゴリズムと暗号鍵により復号化を行い、ルーティング処理手段２３ｂとＬＡＮインタフェース２２ｂを経由し、構内ネットワーク３を介して端末９に転送される。

【００５２】このように、ゲートウェイ装置４における暗号化／復号化処理手段２６ａにて、一部の処理を追加するのみで、新たなＳＡへの対応が可能になる。

【００５３】次に、端末６から端末９のセッションに対するＳＡ有効時間満了による、セッションに対するＳＡの解放処理について説明する。

【００５４】ゲートウェイ装置４における第１のタイマ２７ａは、ＳＡデータベース２４のセッション毎のタイムスタンプを定期的に参照し、ＳＡのタイムスタンプと固定的なＳＡの有効時間と現在の時刻とにより、ＳＡの有効時間満了を算出する。そして、満了であった場合に、当該ＳＡのＳＡＩＤ、送信元アドレス、送信元ポート番号、送信先アドレス、送信先ポート番号、暗号化アルゴリズムなどを含むＳＡ解放指示を鍵交換手段２５ａへ通知する。

【００５５】鍵交換手段２５ａは、セッション鍵交換手順に基づくメッセージを生成した後、パケットヘッダの宛先アドレスに対向となるゲートウェイアドレス（この場合、ゲートウェイアドレスは、ゲートウェイ装置５となる）を記載し、ルーティング処理手段２３ａと暗号化／復号化処理手段２６ａとＷＡＮインタフェース２１を経由して、広域ネットワーク１に転送される。（なお、暗号化／復号化処理手段２６ａにおいては、必ずしも暗号化されなくてもよい。）さらに、セッション鍵交換手順に基づくメッセージを含むパケットは、ゲートウェイ装置５へ転送され、ＷＡＮインタフェース２１ｂ、暗号化／復号化処理手段２６ｂとルーティング処理手段２３ｂを介して、鍵交換手段２５ｂへ転送され、セッション鍵交換手順に基づき、当該セッションに対するＳＡを解放し、ゲートウェイ装置４、５のＳＡデータベースは、図９（ａ），（ｂ）のように更新される。

【００５６】以上説明したように、本実施の形態においては、あるセッションに対する通信内容を暗号化するための通信チャネルであるセキュリティアソシエーションを確立している段階において、セキュリティアソシエーションの有効時間満了までの残余時間が一定時間以下であった場合に、暗号鍵交換手段に対して、そのセッションに対する新たなセキュリティアソシエーションを確立する指示を出すタイマを有し、そのセッションに対する新たなセキュリティアソシエーションを確立すると共に、そのゲートウェイ装置の暗号化処理を施す暗号化／復号化処理手段は、あるセッションに対して、複数のセキュリティアソシエーションが存在する場合には、最新のセキュリティアソシエーションを使用して暗号化処理を行うことことにより、新たなセキュリティアソシエーションへの移行が容易になるという利点を有する。

【００５７】すなわち、一つのセッションに対して、複数のセキュリティアソシエーションが存在する場合には、最新のセキュリティアソシエーションを使用して暗号化処理を行うことことにより、定期的なセッション鍵の交換を行いつつ、定常的かつ連続的にやりとりされるデータの機密性・秘匿性を確保することを容易に実現できるという効果が得られる。

【００５８】以上説明した暗号化通信における、送信側の動作をまとめると図５のようになる。

【００５９】すなわち、まず、鍵交換プロトコル（ＩＫＥ）に基づき、１つのセッションに対するセキュリティアソシエーション（ＳＡ）を確立し、暗号鍵の情報（メッセージ）を通信先に送り、通信先のＳＡデータベース

にＳＡ情報を蓄積する（鍵交換動作）（ステップ５０）。

【００６０】次に、セッションを確立し、パケットを暗号化し、パケットのヘッダにＳＡＩＤを付与して送信する（暗号化通信動作）（ステップ５１）。

【００６１】次に、ＳＡデータベースのセッション毎のタイムスタンプを定期的に参照し、現在の時刻と、予め定められているＳＡ有効期間とを用いてＳＡ有効期限の管理を行う（ＳＡ有効期限管理動作）（ステップ５２）。

【００６２】次に、ＳＡの有効期限が近づくと、新しいセキュリティアソシエーションを確立し、新たな暗号鍵の情報（メッセージ）を通信先に送る（鍵更新動作）（ステップ５３）。

【００６３】次に、ＳＡデータベースを参照し、送信先アドレスと送信ポート番号が一致し、かつ、タイムスタンプが最新であるＳＡを検索し、そのＳＡの暗号化アルゴリズムで暗号化を行い、そのＳＡのＩＤをパケットのヘッダに記載して送信する（暗号化通信動作）（ステップ５４）。

【００６４】そして、旧ＳＡの有効期間が満了すると、そのＳＡを解放する（ＳＡ解放動作）（ステップ５５）。

【００６５】また、暗号化通信における受信側の主要な動作をまとめると、図６のようになる。

【００６６】すなわち、ＳＡデータベースを参照し、受信したパケットのヘッダに記載されているＳＡＩＤと一致するＳＡを検索し、そのＳＡの暗号化アルゴリズムと暗号鍵により復号化を行う（ステップ６０）。

【００６７】そして、送信側からＳＡの解放要求があれば、ＳＡ解放処理を行う（ステップ６１）。

【００６８】以上説明した暗号通信動作を実行させるためのプログラムは、例えば、図１０に示すようなコンピュータシステムに適用できる。

【００６９】図１０のコンピュータシステムは、本体部６０１と、キーボード６０２と、ディスプレイ６０３と、入力装置６０４とを含んで構成されている。

【００７０】そして、暗号通信を行うためのプログラムは、本体部６０１にセットされるＣＤ－ＲＯＭ６０７内や、本体部６０１が内蔵するディスク（メモリ）６０６内，あるいは、回線６０８で接続された他のシステムのディスク６０５内に格納される。

【００７１】以上の説明では、対象鍵（共通鍵）を使用した暗号化を例にとり説明しているが、これに限定されるものではない。つまり、非対称な暗号鍵（公開鍵）の交換でも、本発明を同様に適用可能である。公開鍵は、送信者もしくは受信者が、当事者のみならず第三者に対しても公開されている情報のみに基づき、計算により暗号鍵（復号鍵）を生成するものである。公開鍵を使用する場合でも、セキュリティの信頼性を向上させるために一つのセッション中に、鍵を代える必要がある場合がある。

【００７２】例えば、公開鍵情報（鍵を生成する基礎となる公開されている情報）が複数用意されており、一つのセッションに途中で、復号化において使用するべき公開鍵情報を更新するという事態も想定される。このような場合の公開鍵情報の交換にも、本発明を使用することができる。

【００７３】

【発明の効果】以上説明したように、本発明によれば、一つのセッションの途中において、既存の鍵交換機能を利用して容易に、かつ、シームレスに定期的なセッション鍵の交換を行うことができる。よって、定常的かつ連続的にやりとりされるデータの機密性・秘匿性を常に確保することができる。また、本発明は構成がシンプルであるため、実現が容易である。

【図面の簡単な説明】

【図１】本発明の実施の形態にかかるゲートウエイ装置の構成を示すブロック図

【図２】広域ネットワークを介した暗号通信を行うシステムの全体構成を示す図

【図３】本発明の実施の形態における暗号通信の、全体の動作の概要を示すフロー図

【図４】本発明の実施の形態における、暗号鍵の切り換え動作を説明するための図

【図５】本発明の実施の形態における暗号通信の、送信側の主要な動作を示すフロー図

【図６】本発明の実施の形態における暗号通信の、受信側の主要な動作を示すフロー図

【図７】（ａ）セッション開始当初における送信側のＳＡデータベースの内容の一例を示す図

（ｂ）セッション開始当初における受信側のＳＡデータベースの内容の一例を示す図

【図８】（ａ）セッション鍵の交換時期における送信側のＳＡデータベースの内容の一例を示す図

（ｂ）セッション鍵の交換時期における受信側のＳＡデータベースの内容の一例を示す図

【図９】（ａ）有効期間が満了したセキュリティアソシエーション（ＳＡ）を解放した後の、送信側のＳＡデータベースの内容の一例を示す図

（ｂ）有効期間が満了したセキュリティアソシエーション（ＳＡ）を解放した後の、受信側のＳＡデータベースの内容の一例を示す図

【図１０】コンピュータシステムの構成の一例を示す図

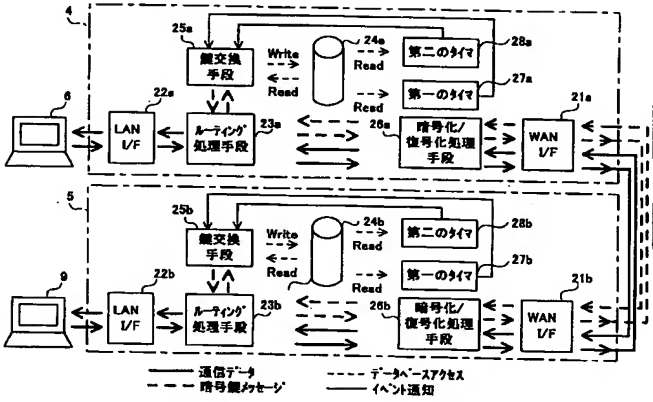
【符号の説明】

１　広域ネットワーク
２，３　構内ネットワーク
４，５　ゲートウェイ装置
６，７，８，９，１０，１１　端末
１２　傍受端末

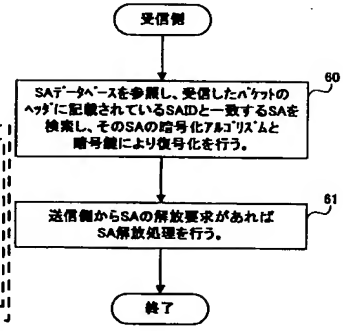
15　　16

２１ａ，２１ｂ　ＷＡＮインタフェース
２２ａ，２２ｂ　ＬＡＮインタフェース
２３ａ，２３ｂ　ルーティング処理手段
２４ａ，２４ｂ　ＳＡ（Ｓｅｃｕｒｉｔｙ　Ａｓｓｏｃｉａｔｉｏｎ）データベース
２５ａ，２５ｂ　鍵交換手段
２６ａ，２６ｂ　暗号化／復号化処理手段
２７ａ，２７ｂ　第一のタイマ
２８ａ，２８ｂ　第二のタイマ

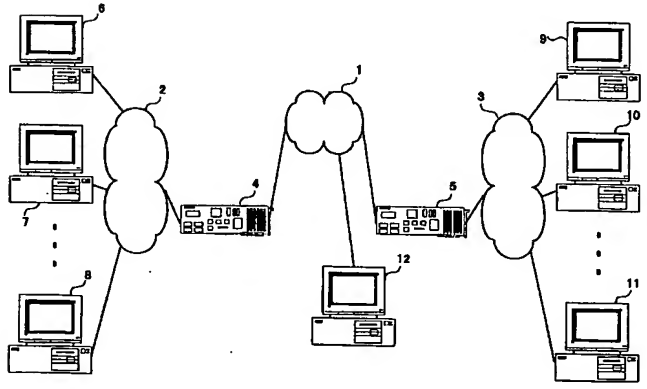
【図１】



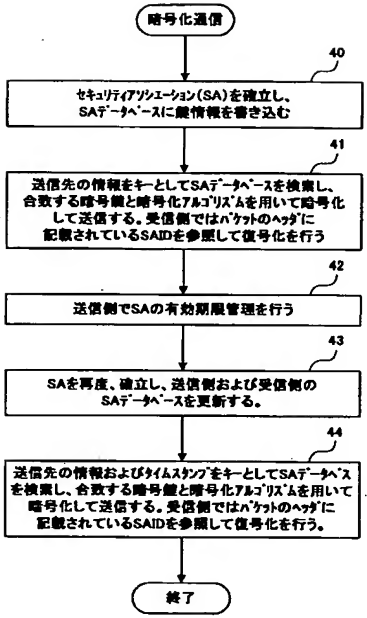
【図６】



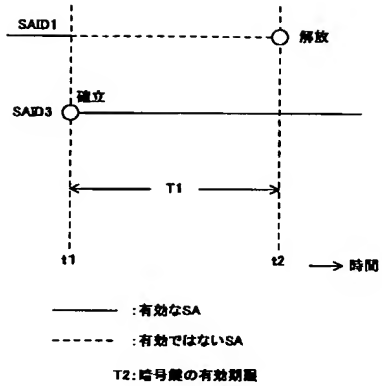
【図２】



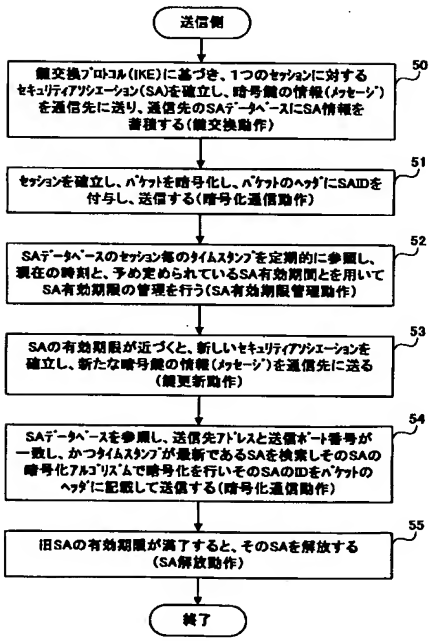
【図３】


暗号化通信
40
セキュリティアソシエーション(SA)を確立し、SAデータベースに鍵情報を書き込む
41
送信先の情報をキーとしてSAデータベースを検索し、合致する暗号鍵と暗号化アルゴリズムを用いて暗号化して送信する。受信側ではパケットのヘッダに記載されているSAIDを参照して復号化を行う
42
送信側でSAの有効期限管理を行う
43
SAを再度、確立し、送信側および受信側のSAデータベースを更新する。
44
送信先の情報およびタイムスタンプをキーとしてSAデータベースを検索し、合致する暗号鍵と暗号化アルゴリズムを用いて暗号化して送信する。受信側ではパケットのヘッダに記載されているSAIDを参照して復号化を行う。
終了

【図４】


SAID1
解放
SAID3
確立
T1
t1
t2
時間
:有効なSA
:有効ではないSA
T2:暗号鍵の有効期限

【図５】


送信側
鍵交換プロトコル(IKE)に基づき、1つのセッションに対するセキュリティアソシエーション(SA)を確立し、暗号鍵の情報(メッセージ)を通信先に送り、通信先のSAデータベースにSA情報を蓄積する(鍵交換動作)
50
セッションを確立し、パケットを暗号化し、パケットのヘッダにSAIDを付与し、送信する(暗号化通信動作)
51
SAデータベースのセッション毎のタイムスタンプを定期的に参照し、現在の時刻と、予め定められているSA有効期間とを用いてSA有効期限の管理を行う(SA有効期限管理動作)
52
SAの有効期限が近づくと、新しいセキュリティアソシエーションを確立し、新たな暗号鍵の情報(メッセージ)を通信先に送る(鍵更新動作)
53
SAデータベースを参照し、送信先アドレスと送信ポート番号が一致し、かつタイムスタンプが最新であるSAを検索しそのSAの暗号化アルゴリズムで暗号化を行いそのSAのIDをパケットのヘッダに記載して送信する(暗号化通信動作)
54
旧SAの有効期限が満了すると、そのSAを解放する(SA解放動作)
55
終了

【図７】

SAID	送信元アドレス	送信元ポート番号	送信先アドレス	送信先ポート番号	暗号化アルゴリズム	暗号鍵	タイムスタンプ
1	2.2.2.6 (端末 6)	8080	3.3.3.9 (端末 9)	8080	3DES	2F7E...	2000.9.25 21:13:15
2	2.2.2.7 (端末 7)	****	3.3.3.10 (端末 10)	****	DES	FF93...	2000.9.25 21:22:43
...	...	...	...	...	...	...	...

(a)

SAID	暗号化アルゴリズム	暗号鍵
1	3DES	2F7E...
2	DES	FF93...
...	...	...

(b)

【図８】

SAID	送信元アドレス	送信元ポート番号	送信先アドレス	送信先ポート番号	暗号化アルゴリズム	暗号鍵	タイムスタンプ
1	2.2.2.6 (端末 6)	8080	3.3.3.9 (端末 9)	8080	3DES	2F7E...	2000.9.25 21:13:15
2	2.2.2.7 (端末 7)	****	3.3.3.10 (端末 10)	****	DES	FF93...	2000.9.25 21:22:43
3	2.2.2.6 (端末 6)	8080	3.3.3.9 (端末 9)	8080	3DES	590A...	2000.9.25 22:13:15
...	...	...	...	...	...	...	...

(a)

SAID	暗号化アルゴリズム	暗号鍵
1	3DES	2F7E...
2	DES	FF93...
3	3DES	590A...
...	...	...

(b)

【図９】

SAID	送信元アドレス	送信元ポート番号	送信先アドレス	送信先ポート番号	暗号化アルゴリズム	暗号鍵	タイムスタンプ
1	2.2.2.7 (端末 7)	****	3.3.3.10 (端末 10)	****	DES	FF93・・・	2000.9.25 21:22:43
2	2.2.2.6 (端末 6)	8080	3.3.3.9 (端末 9)	8080	3DES	590A・・・	2000.9.25 22:13:15
・・・	・・・	・・・	・・・	・・・	・・・	・・・	・・・

(a)

SAID	暗号化アルゴリズム	暗号鍵
2	DES	FF93・・・
3	3DES	590A・・・
・・・	・・・	・・・

(b)

【図１０】